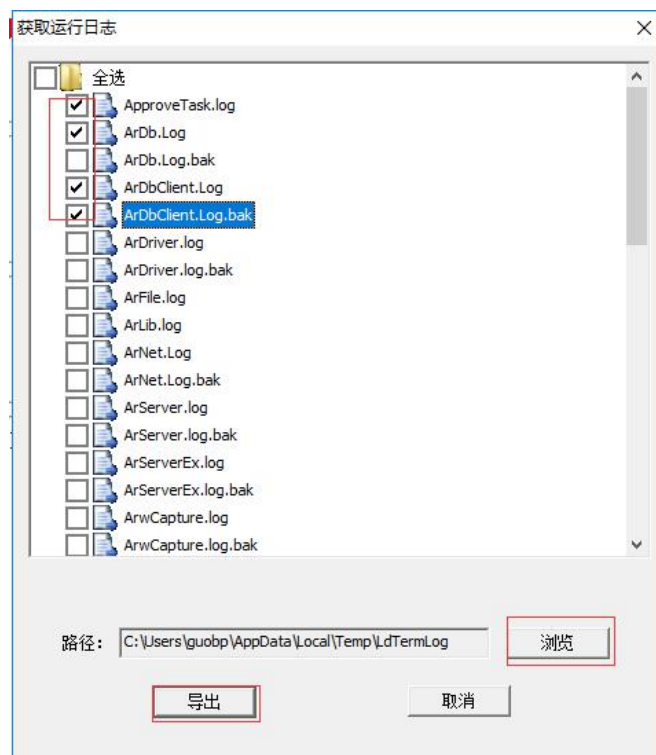


## 绿盾调试工具使用说明（内部人员使用）

- 注意：1、获取日志功能可以给客户（代理）使用；
- 2、该工具隐藏功能需要公司技术人员操作，不能给客户（代理）使用。
- 3、以管理员权限运行程序；

### 一、 获取日志

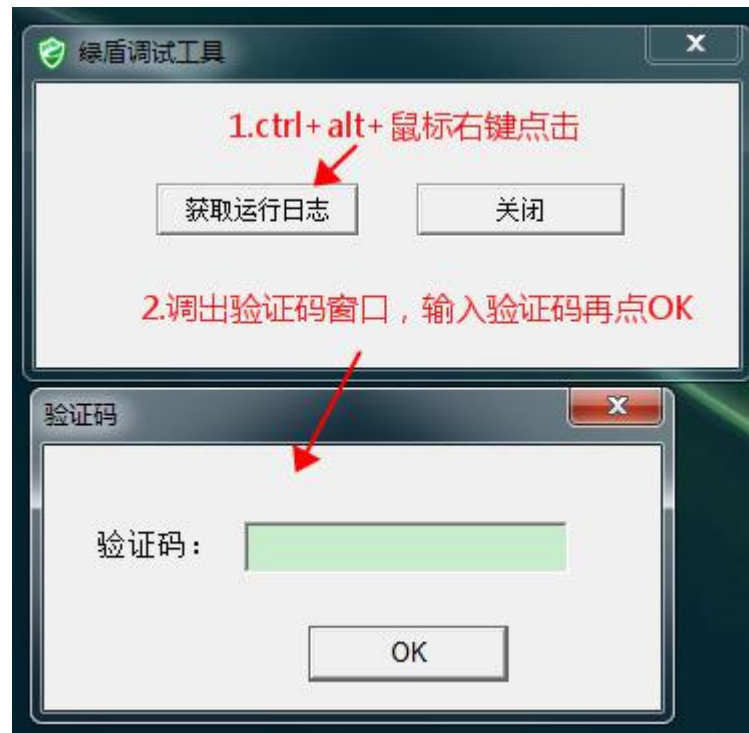


获取完日志，会自动弹出该文件夹，文件夹内的.log 文件就是绿盾运行日志。

### 二、隐藏功能

打开隐藏功能方法：

按住 ctrl+alt+ 鼠标右键， 点击 “获取运行日志”， 弹出验证码窗口（输入密码  
XXXXXXXXXXXXXXXXXX）





### 功能说明：

勾选的时候是关闭该功能，从勾选状态到不勾选状态，功能就会恢复回去。

（一）驱动相关钩子：（必须重启电脑才会生效）

#### 1、卸载 ndis：

32 位系统，会执行 NdisSetup32.exe -uninstall 且 NdisSetup32.exe 改名 NdisSetup32.exe.bak

64 位系统，会执行 NdisSetup64.exe -uninstall 且 NdisSetup64.exe 改名 NdisSetup64.exe.bak

#### 2、关闭加密驱动：

普通版本：LdEIS.sys 改名 LdEIS.sys.bak

三代版本：LDMFilter.sys 改名 LDMFilter.sys.bak

LDMFilter\_32.sys 改名 LDMFilter\_32.sys.bak

LDMFilter\_64.sys 改名 LDMFilter\_64.sys.bak

LDMFilter\_XP.sys 改名 LDMFilter\_XP.sys.bak

会使得系统失去加密解密功能。

### 3、关闭 core 驱动：

LdCore.sys 改名成 LdCore.sys.bak

LdCore32.sys 改名成 LdCore32.sys.bak

LdCore64.sys 改名成 LdCore64.sys.bak

主要在 64 位系统中，会导致很多控制失效，在技术人员指导下使用。

### 4、关闭 Tdi 驱动：

LdTDI.sys 改名 LdTDI.sys.bak

会使得外网功能失效。

（二）加密 hook 相关钩子：（重启终端进程即可）

### 1、关闭加密钩子：

32 位系统：LdSysCtrl.dll

64 位系统：LdHook32.dll

LdHook64.dll

会使得系统一些控制失效，如打印限制、截屏、OLE 等等

### 2、关闭半透明加密：（三代版本组件）

LdSmartEnc32.dll 改名 LdSmartEnc32.dll.bak

LdSmartEnc64.dll 改名 LdSmartEnc64.dll.bak

### 3、关闭右键菜单：

改名安装目录的 LdMenuExt.dll 和 LdMenuPlug.dll、LdMenuPlug\_64.dll

### 4、关闭二代钩子：（绿盾普通版本才有以下组件）

LdSSDTHook32.dll 改名 LdSSDTHook32.dll.bak

LdSSDTHook64.dll 改名 LdSSDTHook64.dll.bak

### 5、关闭加密锁：

改名安装目录的 LdExplorerIcon.dll，并重启 explorer.exe

### 6、关闭屏幕水印：

LdWaterMarkHook32.dll 改名 LdWaterMarkHook32.dll.bak

LdWaterMarkHook64.dll 改名 LdWaterMarkHook64.dll.bak

## 7、关闭智能加密：（三代版本组件）

LdContentAware.dll 改名 LdContentAware.dll.bak

（三）内外网 hook 相关钩子：（重启终端进程即可）

### 1、关闭打印监控：

把 LdPrintMonitor.dll 改名成 LdPrintMonitor.dll.bak

把 LdPrintMonitor64.dll 改名成 LdPrintMonitor64.dll.bak

会导致打印监控功能失效。

### 2、关闭聊天监控：

QQFileMonitor.dll 改名 QQFileMonitor.dll.bak

CapNsg.dll 改名 CapNsg.dll.bak

### 3、关闭内外网：

关闭 LdTermPlug.exe 和 LdTermPlug64.exe 的功能。

（四）其他功能：

### 1、获取运行日志：

获取完日志，会自动弹出该文件夹，文件夹内的.log 文件就是绿盾运行日志。

### 2、重新生成终端编号：（执行完需要重启终端电脑）

32 位系统，会清空 C:\Windows\System32\Dblist.mak 文件中 Guid 项的内容；

64 位系统，会清空 C:\Windows\SysWOW64\Dblist.mak 文件中 Guid 项的内容；

C(绿盾安装所在盘根目录):\Eis\$Bak\Dblist.mak 改名 Dblist.mak1;

### 3、重启绿盾终端：

重启绿盾终端进程。

### 4、打开安装目录：

可以直接打开绿盾终端安装目录

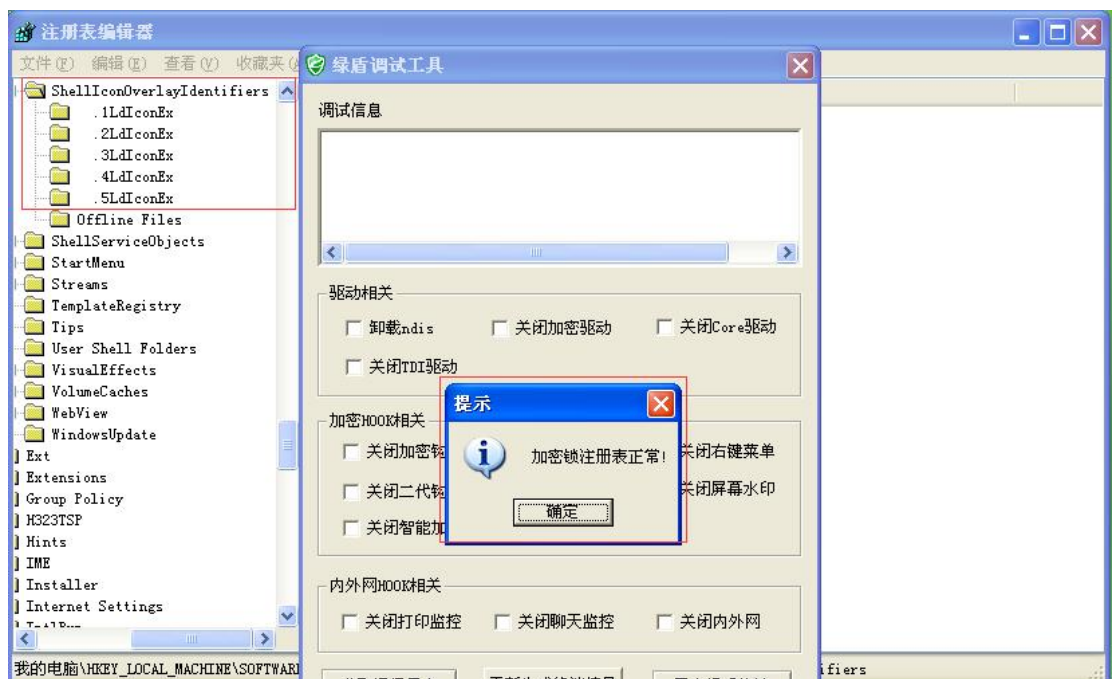
### 5、服务器配置



可修改主服务器和辅服务器对应的 IP 和端口，修改完成后，还需要再点击“重启绿盾终端”。

#### 6、检查加密锁：

主要用于解决注册表加密锁图标排序太后面导致无法显示问题，运行后可使得加密锁注册表那边位置提升上去。



#### 7、导出终端配置：

可以把终端安装目录下 repository 下的 2001-01-01 配置，还有一些 bak 备份配置，全部导出

